STAT

Page Denied

GOVERNMENT COMPUTERNEWS

THE NEWSPAPER SERVING COMPUTER USERS THROUGHOUT THE FEDERAL GOVERNMENT

July 19, 1985 Volume 4 Number 12

Photo by Kenneth Leong Hong

Rep. Dan Glickman (D-Kan.) chairs hearing on computer security.

Security Directive Lambasted

By Eric Fredell
GCN Staff

A diverse group of private and public officials attacked the Reagan administration's computer security directive, arguing it is confusing, possibly illegal and that it inappropriately places responsibility for federal computer security in military hands.

The criticism, which focused on National Security Decision Directive 145, came at a recent hearing held by the House Science and Technology Subcommittee on Transportation, Aviation and Materials.

The directive, signed last September, placed the National Security Agency in charge of assuring security of all federal computers and telecommunications transmitting classified information and other sensitive national security information. It also established an organizational structure to guide safeguarding activities.

Several witnesses questioned the appropriateness of putting defense-minded individuals in charge of security for civilian-agency computers. Rep. Jack Brooks (D-Texas) said the directive is ill-advised and potentially troublesome because it vests in DOD the authority to classify and control information in the civilian sector that it deems critical to national security. "Now that might be the price of butter," Brooks said.

The chairman of the Government Operations Committee said it would be impossible for the department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.

The American Civil Liberties Union, in a prepared statement presented by legislative counsels Allan Adler and Jerry Berman, said the authority given NSA is "an unprecedented, unwise and uncheckable primacy of the nation's national security apparatus in information policy — an area where the balanced consideration of values other than 'security' is of paramount importance to our system of government."

But an NSA official, Walter Deeley, said NSA is a people-oriented agency with a goal of protecting the nation's communications systems. "We are not," said the NSA deputy director of communications security, "a super-secret agency that tries to run over everybody doing our own thing."

Deeley and two other Defense

see Security page 16

Feds Push on as Industry Slumps

Industry Layoffs, Cutbacks Rising

By Peter Hager
GCN Staff

Fiscal 1985 has not been kind to the high technology industry. Tumbling stock prices, revenues and profits have sent computer industry leaders reeling against the ropes to contemplate strategic comebacks while other less-established companies have declared Chapter 11 bankruptcy and left the ring for good.

According to IBM President and Chief Executive Officer John Akers, the company's profits for the first three quarters of 1985 will be less than the same period of 1984

Agencies Miss Potential Savings

By Peter Hager
GCN Staff

The current depression in the computer market has contributed to a bonanza of price reductions on a wide assortment of high-tech hardware. But the government, handcuffed by federal procurement regulations, seems incapable of taking advantage of the big savings.

Many private and commercial computer users are scheduling their purchases to monopolize on the current drop in prices. In the present buyer's market, where industry giant IBM has lowered prices 6 to 20

Ore. VDT Bill Vetoed

By Chris Tlustos
GCN Staff

Oregon Governor Victor Atiyeh

"There are statutes and rules on the Oregon books that deal in general with alleged hazards in the automated workplace," Miles

DOD Reps Urge Central ADP Security Control

Security from page 1

Department officials, Donald C. Latham, assistant secretary of defense for Command, Control, Communications and Intelligence, and Robert L. Brotzman, director of the Defense Computer Security Center, emphasized the threat to the United States of inadequate security measures.

Latham said the country is being "bled to death," while Brotzman said U.S. adversaries can cause a great deal of damage with little effort or expense.

Part of the concern raised by the directive's critics stemmed from the strong representation of the defense agencies on the committees established by NSDD 145. One, the National Telecommunications and Information Systems Security Committee, which Latham chairs, has 10 DOD representatives on its 22-member panel.

When asked to respond to criticisms that the committee is heavily defense-oriented, Latham said, "I don't think that criticism is well-based. I don't believe it is a military-dominated committee at all." He also called the committee well-balanced.

Brooks also argued the administration had no legal authority to create a national policy for telecommunications and computer systems. He said policies of such importance must include public hearings and a full debate in the Congress.

Rep. Dan Glickman (D-Kan.), who called the hearing and serves as the subcommittee chairman, also expressed concern. "I'm more concerned about the process and how that thing [NSDD 145] got into implementation than I am with substance," Glickman said following the hearing. "No one seems to know how this was done."

Latham said all the appropriate civilian agencies were well represented at meetings concerning the directive.

Warren Reed, director of the General Accounting Office's Information Management and Technology Division, said the directive is unclear in some areas. Specifically, Reed said, NSDD 145 established a sensitive but unclassified category of information without clearly defining the types of information that would be included in this category.

Reed also said the directive may cause confusion with existing statutes, including the Brooks Act and the Paperwork Reduction Act. While the National Bureau of Standards is currently charged with issuing computer security standards, and the Office of Management and Budget develops and implements government computer security programs, Reed said it is unclear how these policies and the new directive fit together.

Photo by Kenneth Leong Hong

Donald Latham, DOD Assistant Secretary

Brooks made a similar but much more direct statement, arguing it is in conflict with existing statutes. "In issuing NSDD 145, the president ignored the statutory authorities and unilaterally transferred these responsibilities to DOD," he said. He said Reagan should have proposed legislation to effect this change legally.

Latham, Deeley and Brotzman each emphasized the importance of centralizing control of computer security. Deeley said DOD already sets communications security for the government. Adding computer security to that responsibility, he said, "is in line with the trend in technology which blurs the distinction between telecommunications systems and automated information systems. "

Although Glickman and Brooks did not say what action would be taken as a result of the hearing, the two, along with several others, introduced legislation later that day that would establish computer security training programs within government agencies.

Bill Proposes ADP Security Training

A bill introduced shortly after the conclusion of a congressional hearing on government computer security would establish a training program for federal ADP personnel.

Rep. Dan Glickman (D-Kan.) introduced the Computer Security Research and Training Act of 1985 within hours of concluding a hearing at which National Security Decision Directive 145 was heavily criticized. NSDD 145 puts the National Security Agency, an intelligence branch of the Defense Department, in charge of computer security for both military and civilian agencies [see related article, pg. 1].

The legislation would authorize the National Bureau of Standards to do background research, including a vulnerability assessment of government systems, and develop training guidance so that agencies can train their ADP personnel to secure government computer systems properly. All agencies would be required to provide computer security training on a periodic basis. The initial costs of the program are estimated at $1 million.

"What we propose is some preventative medicine — a means of problem avoidance," Glickman said at a press conference where he announced he would introduce the legislation. "The reason we're doing this is because we perceive a real and growing vulnerability of these systems, and we want to do something about it before a major breach occurs," he said.

The bill co-sponsors include the chairman of the House Science and Technology committee, Rep. Don Fuqua (D-Fla.), and the chairman of the House Government Operations Committee, Rep. Jack Brooks (D-Texas). The bill has been sent to both committees, and Brooks said he expects it will receive "a warm reception."

"Computer security has remained a low priority for most federal agencies, and a relatively small amount of funds are devoted to this area," Brooks said.

Investigations of federal agencies that his committee conducted found computer security lax in almost every case and in some cases virtually non-existent, he said.

VDT Bill Said Unneeded

ressed included de-